

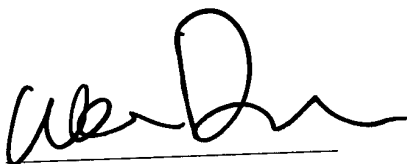


TRANSPERFECT | TRANSLATIONS

City of New York, State of New York, County of New York

ATLANTA
BOSTON
CHICAGO
DALLAS
FRANKFURT
HOUSTON
LONDON
LOS ANGELES
MIAMI
MINNEAPOLIS
NEW YORK
PARIS
PHILADELPHIA
SAN DIEGO
SAN FRANCISCO
SEATTLE
WASHINGTON, DC

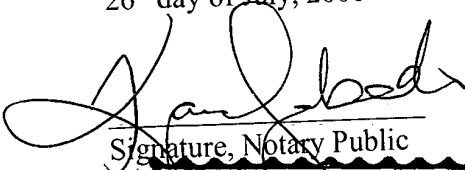
I, Wendy Dorsett, hereby certify that the following is, to the best of my knowledge and belief, a true and accurate translation of the attached Patent Opinion and Response (Client File Number 1196.GLE.PT) from German to English.



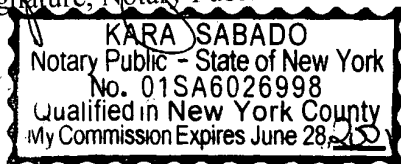
Wendy Dorsett

Sworn to before me this

26th day of July, 2000



Signature, Notary Public



Stamp, Notary Public

Gleiss & Große
Patentanwälte Rechtsanwälte
München Stuttgart

Patentanwälte Gleiss & Große D-70469 STUTTGART

Europäisches Patentamt

80298 MÜNCHEN

Dr. jur. Alf-Olav Gleiss, Dipl.-Ing. PA
Rainer Große, Dipl.-Ing. PA
Dr. Andreas Schrell, Dipl.-Biol. PA
Dr. Frhr. v. Uexküll, Dipl.-Chem. PA
Torsten Armin Krüger RA
Dr. Wilhelm Heuer, Dipl.-Phys. PA
Torsten Bettinger, LL. M. RA

PA: Patentanwalt
European Patent Attorney
European Trademark Attorney
RA: Rechtsanwalt, Attorney-at-law

D-70469 STUTTGART
MAYBACHSTRASSE 6A
Telefon: +49(0)711 81 45 55
Telefax: +49(0)711 81 30 32
Telex: 72 27 72 jura d
e-mail: jurapat@aol.com

D-80469 MÜNCHEN*
MORASSISTRASSE 20
Telefon: +49(0)89 21578080
Telefax: +49(0)89 21578080
e-mail: GGpat@aol.com

In cooperation with
Shanghai Hua Dong Patent Agency
Shanghai, China

Rückantwort nach/Reply to:

STUTTGART

18. Oktober 1999
SC-ne

PCT-Anmeldung PCT/EP98/06769
Anmelder: Brokat Infosystems AG et al.

Unsere Akte: 22738 WO

— JURAPAT —

— JURAPAT —

Auf den Bescheid vom 13. August 1999

Anliegend wird ein neuer Anspruchssatz mit den Ansprüchen 1 bis 12 und Austauschseiten 4, 5, 6 und 6a der Beschreibung in 2-facher Ausfertigung eingereicht.

1. Änderungen in den Ansprüchen

Der neue Anspruch 1 entspricht dem Gegenstand der ursprünglichen Ansprüche 1 und 3, wobei der Oberbegriff gemäß D1 abgefasst wurde sowie Bezugszeichen eingeführt wurden.

Die neuen Ansprüche 2 und 4 bis 11 entsprechen den ursprünglichen Ansprüchen 2 und 4 bis 11.

Der neue Anspruch 3 entspricht einer bevorzugten Variante des ursprünglichen Anspruchs 3.

Der neue Anspruch 12 entspricht dem Gegenstand des ursprünglichen Anspruchs 15, wobei gemäß des ursprünglichen Verfahrensanspruchs 3 klargestellt wurde, dass die vom Mobilfunktelefon 7 empfangene Nachricht über das Telefonnetz empfangen wurde.

2. Änderungen in der Beschreibung

In der Beschreibung wurde den Einwänden der Prüfungsstelle Rechnung getragen und die Dokumente D1 und D2 gewürdigt sowie die Beschreibung an die geltende Anspruchsfassung angepasst.

3. Patentfähigkeit des neuen Anspruchs 12 (vormaliger Anspruch 15)

Ein wesentlicher Unterschied zu der Offenbarung von D1 ist, dass gemäß der vorliegenden Erfindung eine Übertragung einer zu signierenden Nachricht über ein Telefonnetz aus einer externen Quelle erfolgt, während in D1 die Nachricht im Mobiltelefon oder einem direkt angeschlossenen Gerät (Smartcard) erzeugt wird. Eine Übertragung einer zu signierenden Nachricht erfolgt in D1 nicht. D1 offenbart also nicht, dass über ein Telefonnetz eine zu signierende Nachricht übermittelt wird. Diesem Sachverhalt trägt der neue Anspruch 12

Rechnung. Ihm kommt daher Neuheit und erfinderische Tätigkeit zu.

Dr. Andreas Schrell
European Patent Attorney

Anlagen:

Ansprüche 1 bis 12 (2-fach)

Seiten 4 bis 6a der Beschreibung (2-fach)

mit der Rechner-Tastatur unter Umgehung der Rechner-Software verbunden. Die Signatur wird im Signiergerät erzeugt. Je mehr Aufgaben dabei von der Rechner-Software übernommen werden und je weniger das Signiergerät leisten muss, desto kostengünstiger ist das Verfahren.

Die WO 96/32700 offenbart ein Verfahren gemäß dem eine in einem Mobilfunktelefon erzeugte Nachricht digital signiert und weitergeleitet wird. Die EP 0 689 316 A2 offenbart ein Verfahren und eine Einrichtung zur Identifizierung und Verifizierung von Daten in einem Kommunikationsnetzwerk.

Grundsätzlich besteht in all diesen Ausführungsformen jedoch das Problem, dass genau die Daten signiert werden müssen, die der Benutzer signieren möchte. Es muss also ausgeschlossen werden, dass ein Virus beispielsweise die Daten während der Übertragung von der Darstellungskomponente, zum Beispiel dem Display, an die Signierkomponente, zum Beispiel den Kryptoprozessor, verändert. Ferner muss sichergestellt werden, dass eine Geheimzahl (zum Beispiel PIN), die zur Auslösung der Signaturen notwendig ist, nicht von anderen Programmen von der Tastatur mitgelesen werden kann und Dritten bekannt wird.

Zudem wird der möglichst flächendeckende Einsatz der Möglichkeit zur digitalen Signatur durch die vergleichsweise geringe Verbreitung von Signiergeräten eingeschränkt. In potentiellen Anwendungsbereichen digitaler Signaturen, wie beispielsweise dem Internet-Banking, müsste demgemäß eine kosten

aufwendige Infrastruktur zur Verbreitung der Signiergeräte geschaffen werden. Problematisch ist dabei auch die Installation von Signiergeräten am Rechner. Einerseits müssen die Geräte physikalisch mit dem Rechner verbunden werden, wobei die seriellen Schnittstellen eines PC häufig bereits belegt sind. Alternative Verfahren zur Anbindung der Signiergeräte an Rechner sind ebenfalls problematisch, da hierfür zumindest die Installation von Software-Treibern und manchmal auch von zusätzlicher Hardware notwendig ist. Zusätzlich müssen für alle Signiergeräte häufig spezielle Software-Komponenten installiert werden, die es dem Anwendungsprogramm erlauben, mit dem Signiergerät zu kommunizieren.

Ein weiteres Problem der herkömmlichen Verfahren zur digitalen Signatur besteht darin, dass diese standortabhängig sind. Bestimmte Anwendungsbereiche für den Einsatz digitaler Signaturen, wie beispielsweise das Internet-Banking, sind aufgrund überall zugänglicher öffentlicher Internet-Terminals standortunabhängig. Würden diese Internet-Banking-Anwendungen nun mit den bekannten standortabhängigen Verfahren zur digitalen Signatur kombiniert werden, wäre die Standortunabhängigkeit dieser Anwendungsbereiche verloren.

Das der vorliegenden Erfindung zugrundeliegende technische Problem besteht also darin, ein kostengünstiges, leicht zu realisierendes und standortunabhängiges Verfahren zum digitalen Signieren von Nachrichten sowie dafür geeignete Vorrichtungen bereitzustellen.

Dieses technische Problem wird durch die Lehre gemäß Hauptanspruch gelöst. Die Erfindung sieht demgemäß ein Verfahren zum digitalen Signieren einer an eine Empfangsvorrichtung zu übertragenden Nachricht mittels eines Signiergerätes vor, wobei die zu signierende Nachricht von einer Sendevorrichtung an eine Empfangsvorrichtung, diese Nachricht anschließend von der Empfangsvorrichtung über ein Telefonnetz, insbesondere ein Mobilfunktelefonnetz, an ein der Sendevorrichtung zugeordnetes Signiergerät übertragen wird, diese Nachricht sodann im Signiergerät signiert und an die Empfangsvorrichtung als signierte Nachricht zurückübertragen wird. In besonders bevorzugter Ausführungsform der Erfindung ist das Signiergerät ein Mobilfunktelefon und das Telefonnetz dementsprechend das Mobilfunktelefonnetz.

Im Zusammenhang mit der vorliegenden Erfindung wird unter einem digitalen Signieren einer Nachricht ein Vorgang verstanden, bei dem auf elektronischem Wege der Wille zur Abgabe und der Inhalt einer Nachricht bestätigt wird. Dies geschieht durch partielle oder vollständige Verschlüsselung der zu signierenden Nachricht oder durch Verschlüsselung einer kryptographischen Prüfsumme dieser Nachricht in eine signierte Nachricht mittels eines geheimen Schlüssels unter Anwendung eines mathematischen Verfahrens. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer signierten Nachricht entweder die signierte Nachricht als ganze oder die Signatur selbst verstanden. Die Signierung dient dazu, später eine Authentifizierung des Nutzers durchführen

zu können. Im Zusammenhang mit der vorliegenden Erfindung wird also unter einer signierten Nachricht auch nur die elektronisch erzeugte Signatur der Nachricht verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer Nachricht jegliche Art von in elektronischer Form wiedergegebbarer Information, beispielsweise Zahlen, Buchstaben, Zahlenkombinationen, Buchstabenkombinationen, Grafiken, Tabellen etc. verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einem Signiergerät eine Einheit verstanden, die eine Si-

Gleiss & Große

Patentanwälte Rechtsanwälte
München Stuttgart

PCT/EP98/06769

Anm.: BROKAT INFOSYSTEMS AG....

22738 SC-ne

18. Oktober 1999

Ansprüche

1. Verfahren zum digitalen Signieren einer an eine Empfangsvorrichtung zu übertragenden Nachricht mittels eines Signiergeräts, dadurch gekennzeichnet, dass die zu signierende Nachricht (3) von einer Sendevorrichtung (1) an eine Empfangsvorrichtung (5), diese Nachricht anschließend von der Empfangsvorrichtung (5) über ein Telefonnetz an ein der Sendevorrichtung (1) zugeordnetes Signiergerät übertragen wird, diese Nachricht sodann im Signiergerät signiert und an die Empfangsvorrichtung (5) als signierte Nachricht (9) zurückübertragen wird.
2. Verfahren nach Anspruch 1, wobei das Signiergerät ein Mobilfunktelefon (7) ist.
3. Verfahren nach Anspruch 2, wobei das Telefonnetz ein Mobilfunktelefonnetz ist.
4. Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Signierung ein Public-Key-Verfahren eingesetzt wird, insbesondere ein Public-Key-Verfahren, bei dem die Sendevorrichtung (1) über

einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung (5) über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachrichten zwischen Empfangsvorrichtung (5) und Mobilfunktelefon (7) mittels des Short-Message-Service (SMS) übertragen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht (3) vor der Signierung mittels einer im Mobilfunktelefon (7) vorgesehenen Anzeigeeinrichtung (13) dargestellt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel über eine Tastatureinrichtung des Mobilfunktelefons (7) eingegeben wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons (7) abgelegt ist, und dieser Schlüssel mittels einer über eine Tastatureinrichtung des Mobilfunktelefons (7) eingebbaren Geheimzahl (PIN) freigegeben wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Chip-Karte die Erstellung der signierten Nachricht (9) durchführt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon (7) die Erstellung der signierten Nachricht (9) durchführt und wobei der geheime Schlüssel aus der Chip-Karte (25) gelesen wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon (7) zusätzlich als Sender zur Übermittlung der signierten Nachricht (9) an die Empfangsvorrichtung (5) dient.

12. Chip-Karte für ein Mobilfunktelefon, wobei die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die eine Speichereinheit (27) zur Speicherung des für die Erstellung der signierten Nachricht (9) notwendigen geheimen Schlüssels aufweist, dadurch gekennzeichnet, dass die Signiervorrichtung (21) aus einer vom Mobilfunktelefon (7) über das Telefonnetz empfangenen zu signierenden Nachricht (3) eine signierte Nachricht (9) erstellt.

CONTRACT ON INTERNATIONAL COOPERATION IN THE FIELD OF PATENTS

Sender: AUTHORITIES ENTRUSTED WITH THE INTERNATIONAL
PRELIMINARY EXAMINATION

[stamp]

<p>[stamp]</p> <p>GLEISS & GROSSE Maybachstrasse 8a D-70469 STUTTGART GERMANY</p>		<p>Gleiss & Grosse Patent Attorneys</p> <p>AUG. 17, 1999 Processed: [initials]</p>	<p>CT</p> <p>[handwritten] 11/13/99 [illegible] 10/1/99 [illegible]</p> <p>WRITTEN DECISION (RULE 66 PCT) [handwritten]: new date: [circled] 2216</p>	<p>RECD JUL 21, 1999</p> <p>WIPO PCT</p>
<p>Date sent (day/month/year) 19/07/99 [illegible date]</p>		<p>ANSWER DUE within 3 months from the above date of dispatch</p>		
<p>File reference of the applicant or lawyer 22738 WO</p>	<p>International file reference PCT/EP98/06769</p>	<p>International filing date (day/month/year) 10/24/1998</p>	<p>Date of priority (day/month/year) 28/10/1997</p>	
<p>International patent classification (IPC) or national classification and IPC H04L9/32</p>				
<p>Applicant BROKAT INFOSYSTEMS AG et al.</p>				

<p>1. This decision is the first written decision of the authorities entrusted with the international preliminary examination</p>																	
<p>2. This decision contains information on the following items:</p> <table border="0"> <tr> <td>I</td> <td><input checked="" type="checkbox"/> basis for the decision</td> </tr> <tr> <td>II</td> <td><input type="checkbox"/> priority</td> </tr> <tr> <td>III</td> <td><input type="checkbox"/> no issuance of a report on novelty, inventive activity, and the commercial applicability;</td> </tr> <tr> <td>IV</td> <td><input type="checkbox"/> lack of unity of the invention</td> </tr> <tr> <td>V</td> <td><input checked="" type="checkbox"/> justified findings acc. to Rule 66.2 (a)(II) with regard to the novelty, the inventive activity and the commercial applicability; documents and statements to support these findings</td> </tr> <tr> <td>VI</td> <td><input type="checkbox"/> Certain stated documents</td> </tr> <tr> <td>VII</td> <td><input checked="" type="checkbox"/> Certain defects in the international application</td> </tr> <tr> <td>VIII</td> <td><input type="checkbox"/> Certain remarks on the international application</td> </tr> </table>		I	<input checked="" type="checkbox"/> basis for the decision	II	<input type="checkbox"/> priority	III	<input type="checkbox"/> no issuance of a report on novelty, inventive activity, and the commercial applicability;	IV	<input type="checkbox"/> lack of unity of the invention	V	<input checked="" type="checkbox"/> justified findings acc. to Rule 66.2 (a)(II) with regard to the novelty, the inventive activity and the commercial applicability; documents and statements to support these findings	VI	<input type="checkbox"/> Certain stated documents	VII	<input checked="" type="checkbox"/> Certain defects in the international application	VIII	<input type="checkbox"/> Certain remarks on the international application
I	<input checked="" type="checkbox"/> basis for the decision																
II	<input type="checkbox"/> priority																
III	<input type="checkbox"/> no issuance of a report on novelty, inventive activity, and the commercial applicability;																
IV	<input type="checkbox"/> lack of unity of the invention																
V	<input checked="" type="checkbox"/> justified findings acc. to Rule 66.2 (a)(II) with regard to the novelty, the inventive activity and the commercial applicability; documents and statements to support these findings																
VI	<input type="checkbox"/> Certain stated documents																
VII	<input checked="" type="checkbox"/> Certain defects in the international application																
VIII	<input type="checkbox"/> Certain remarks on the international application																
<p>3. The registrant is requested to comment on this decision</p> <p>When? See above-specified deadline. The applicant may apply for an extension from the authorities before the deadline expires. See Rule 66.2 d)</p> <p>How? By submitting a written statement, and if applicable, changes in accordance with Rule 66.3. See Rule 66.8 and 69.9 on the form and language.</p> <p>Cf.: See Rule 66.4 with respect to an additional option for submitting changes See Rule 66.4 with respect to the obligation of the examiner to take into account changes and/or counterproposals See Rule [illegible]6.6 with respect to an informal discussion with the examiner</p> <p>If no statement is submitted, the international preliminary inspection report will be issued on the basis of this decision.</p>																	
<p>4. Date on which the international preliminary examination report must be issued, in accordance with Rule 69.2, is: February 28, 2000, at the latest.</p>																	
<p>Name and mailing address of the authorities entrusted with the international preliminary examination:</p> <p>Europäisches Patentamt D-80298 Munich Tel. (+49-89) 2399-0 Telex. 523658 epmu d Fax: (+49-89) 2399 4485</p>	<p>Authorized employee/Examiner</p> <p>Haas. H [logo]</p> <p>Formalities Examiner (incl. extension of deadline) Ahrens, R Tel. (+49-89) 2399 8138</p>																

1. Basis for the decision

1. This decision was issued on the basis of *(replacement information sheets that were submitted to the PCT receiving office upon a request in accordance with Article 14 are deemed "originally submitted" within the scope of this decision.)*:

Description, pages:

1-17 original version

Patent claims, no.:

1-15 original version

Drawings, sheets:

1/3-3/3 original version

2. The following documents have been omitted on account of the changes:

<input type="checkbox"/>	description	pages
<input type="checkbox"/>	claims	no.
<input type="checkbox"/>	drawings	sheet

3. This decision was issued without taking into account (some of) the changes because for the reasons specified, in the opinion of the authorities, these go beyond the disclosure in the originally submitted version (Rule 70.2 (c)):

4. Any additional remarks:

V. Justified findings according to Rule 66.2(a)(ii) with regard to the novelty of the inventive activity and of the commercial applicability: documents and statements to support these findings

1. Findings

Novelty (N)	Claims	12-15
Inventive activity (IS)	Claims	1,2, 12-15
Commercial applicability (IA)	Claims	

2. Documents and statements
see insert

WRITTEN DECISION

International ref. no. PCT/EP98/06769

VII. Particular deficiencies of the international application

It was determined that the international application exhibits the following deficiencies in form or content:

see insert

SECTION V

The current Claim 1 relates to the transmission to a signing device, by means of a telephone network, of a message to be signed.

From the description on pages 14 to 17, it follows that at least all the features mentioned in Claim 3 of the application are essential for the definition of the invention.

Since Claim 1 does not contain these features, it does not conform to the requirement of Article 6 PCT, in conjunction with Rule 6.3 b) PCT, that each independent claim must contain all technical features that are essential for the definition of the invention.

Furthermore, a transmission through a telephone network of a message to be signed would only be a simple, expert measure, which does not involve any inventive step.

The use of a mobile telephone as a signing device in accordance with Claim 2 is already known from D1 (see D1, page 3, lines 22-23).

As for the subject of the independent claims 12 and 14, document D1 (WO-A-96 32700) reveals a mobile telephone or an appropriate chip card for signing a message (see D1, page 2, line 26 - page 3, line 26).

The present Claims 12 and 15 consequently do not fulfill the requirements as set forth in Article 33(2) PCT (novelty).

Even if it were asserted that the device in accordance with patent claims 12 and 14 is new, the subject of the mentioned claims does not involve an inventive step, if one were to consider document D1, particularly since the same subject and the same type of solution are revealed in this document as in the present application.

This also applies to the additional features of the independent claims 13 to 15 (see D1, page 8, lines 1-22).

SECTION VII



In order for the requirements of Rule 5.1(a)ii) to be fulfilled, the documents D1 and D2 (EP-A-0 689 316) are to be specified in the description; the relevant prior art contained therein should be summarized.

In order for the requirements of Rule 6.3 b) PCT to be fulfilled, Claim 1 should be drafted in two parts; the features that, in combination with one another, belong to prior art (see above), are to be included in the preamble of the claim.

The features of the claims should be provided with reference numbers set in brackets (Rule 6.2 b) PCT).

Furthermore, the applicant should adapt the specification to the new claims; in the revision of the application, particularly of the introductory portion, including the presentation of the task or of the advantages of the invention, it should be noted that no facts that extend beyond the content of the application as filed originally will be added (Article 34(2)(b) PCT).

Furthermore, it is stated that the term "in particular" (see Claim 3) does not result in any technical constraints.

  TX FAX	EPA/EPO/OEB D- 80298 Munich 089/2398-0 523 858 apmu d +49 89/2399-4465	Europäisches Patentamt	European Patent Office	Office européen des brevets
		Generaldirektion 2	Directorate General 2	Direction Générale 2

Correspondence with the EPA for PCT Chapter II applications

To ensure that your PCT Chapter II application is handled as quickly as possible, you are requested to use the attached stickers in all the correspondence for the EPA Munich.

One of these stickers should be placed on a well-visible location on the upper edge of the title page of the particular letter.

Gleiss & Große
Patent Attorneys Attorneys-at-Law
Munich Stuttgart

Dr. jur. Alf-Olav A.O. Gleiss, Dipl.-Ing., Patent Attorney
Rainer Große, Dipl.-Ing.
Dr. Andreas Schrell, Dipl.-Biol., Patent Attorney
Dr. Frhr. v. Uexküll, Diplo.-Chem, Patent Attorney
Torsten Armin Krüger, Attorney
Dr. Wilhelm Hauer, Dipl. Phys.
Torsten Bettinger, LL.M. Attorney

PA: Patent attorney
European Patent Attorney
European Trademark Attorney
RA: Attorney, Attorney-at-law

Gleiss & Große Patent Attorneys 70469 STUTTGART

EUROPEAN PATENT OFFICE

80298 MUNICH

70469 STUTTGART
MAYBACHSTRASSE 6A
Telephone: +49(0)711 81 45 55
Fax: +49(0)711 81 30 32
Telex: 72 27 72 jura d
e-mail: jurapat@aol.com

D-80469 MUNICH
MORASSISTRASSE 20
Telephone: +49(0)89 2157 8080
Fax: +49(0)89 2157 8090
e-mail: GGpat@aol.com

In cooperation with
Shanghai Hua Dong Patent Agency
Shanghai, China

Reply to:

STUTTGART

October 18, 1999
SC-ne

PCT application PCT/EP98/06769
Applicant: Brokat Infosystems AG et al.

Our file: 22738 WO

JURAPAT

JURAPAT

On the decision dated August 13, 1999

Enclosed is a new set of claims with Claims 1 to 12 and replacement pages 4, 5, 6 and 6a of the description being submitted in duplicate.

1. Changes in the Claims

The new Claim 1 corresponds to the subject of the original Claims 1 and 3, with the preamble of the claim drafted in accordance with D1 and reference numbers introduced.

The new Claims 2, and 4 to 11, correspond to the original Claims 2, and 4 to 11.

The new claim 3 corresponds to a preferred variant of the original Claim 3.

The new Claim 12 corresponds to the subject of the original Claim 15, where it was explained in accordance with the original Method Claim 3 that the message received by the radio mobile telephone 7 was received through the telephone network.

2. Changes in the Specification

The objections of the examination department were given weight in the specification and Documents D1 and D2 were evaluated; the specification was also adapted to the valid version of the claim.

3. Patentability of the New Claim 12 (formerly claim 15)

An essential difference to the revelation of D1 is that in accordance with the present invention, a transmission of a message to be signed takes place through a telephone network from an external source, while in D1, the message is generated in the mobile telephone or in a directly connected device (Smartcard). A transmission of a message

to be signed does not take place in D1. D1 therefore does not reveal that a message to be signed is transmitted through a telephone network. The new Claim 12 gives weight to these facts. It is therefore entitled to novelty and inventive activity.

[signature]

Dr. Andreas Schrell
European Patent Attorney

Enclosures:

Claims 1 to 12 (duplicate) /

Pages 4 to 6a of the specification (duplicate)/

[incomplete sentence] The signature is generated in the signing device. The more tasks are assumed in the process by the computer software and the less the signing device must accomplish, the more reasonably priced the method is.

The WO 96/32700 reveals a method, according to which a message generated in a mobile radio telephone is digitally signed and transmitted. The EP 0 689 316 A2 reveals a method and a device for identifying and verifying data in a communication network.

In all these forms of embodiment, however, the basic problem is that the data that the user would like to sign is precisely the data that must be signed. The chance, for example, of a virus changing the data during the transmission from the presentation components, e.g., the display, to the signing component, e.g., the cryptoprocessor, must therefore be ruled out. Furthermore, it must be ensured that a secret number (e.g., a PIN), which is required to release the signing, cannot be read by other programs through the keyboard and be known by third parties.

Moreover, the use, which should be as exhaustive as possible, of the capability for digital signing is limited by the comparably modest spread of signing devices. In potential areas of application for digital signatures, such as Internet banking, for instance, a costly infrastructure

would have to be put up to spread the signing devices. In this regard, the installation of signing devices at the computer also presents a problem. On the one hand, the devices must be physically connected with the computer, where the serial interfaces of a PC are often already occupied. Alternative methods for connecting the signing devices to the computer are likewise problematic since this requires at least the installation of software drivers, and sometimes also of additional hardware. In addition, special software components that allow the application program to communicate with the signing device must often be installed for all signing devices.

A further problem of the conventional method for digital signature exists in the fact that these are site-dependent. Certain areas of application for the use of digital signatures, such as Internet banking, are site-dependent on account of the public Internet terminals that can be accessed everywhere. If these Internet banking applications were now to be combined with the known, site-dependent method for digital signing, the site-independence of these areas of application would be lost.

The technical problem, which the present invention seeks to solve, therefore lies in making available a reasonably priced, easy-to-implement and site-independent method for digital signing of messages as well as the devices suitable for these.

This technical problem is solved by the directive in accordance with the main claim. The invention accordingly provides a method for digital signing of a message to be transmitted to a receiving device by means of a signing device, with the message to be signed being transmitted from a sending device to a receiving device, this message subsequently being transmitted from the receiving device through a telephone network, in particular a mobile radio telephone network, to a signing device allocated to the sending device, this message then being signed in the signing device and transmitted back to the receiving device as a signed message. In a particularly preferred embodiment of the invention, the signing device is a mobile radio telephone and the telephone network is correspondingly the mobile radio telephone network.

In connection with the present invention, a digital signing of a message is understood as a process, in which the intention to deliver and the content of a message is confirmed electronically. This takes place through partial or complete encoding of the message to be signed or through encoding of a cryptographic check sum of this message into a signed message by means of a private code, using a mathematical procedure. In connection with the present invention, a signed message is understood as either the signed message as a whole or the signature itself. The signing can later be used to perform an authentication of

the user. In connection with the present invention, a signed message is therefore also understood only as the electronically generated signature of the message. In connection with the present invention, a message is understood as all types of information, for example, numbers, letters, number combinations, letter combinations, graphics, tables, etc., that can be reproduced in electronic form. In connection with the present invention, a signing device is understood as a unit, which [text cut off].

Gleiss & Große
Patent Attorneys Attorneys-at-Law
Munich Stuttgart

PCT/EP98/06769

22738 SC-ne

Applicant: BROKAT INFOSYSTEMS AG. ...

October 18, 1999

Claims

1. Method for digital signing of a message to be transmitted to a receiving device by means of a signing device, characterized in that the message (3) to be signed is transmitted from a sending device (1) to a receiving device (5), this message subsequently transmitted from the receiving device (5) through a telephone network to a signing device allocated to the sending device (1), this message then being signed in the signing device and transmitted back to the receiving device (5) as a signed message (9).
2. Method according to Claim 1, where the signing device is a mobile radio telephone (7).
3. Method according to Claim 2, where the telephone network is a mobile radio telephone network.
4. Method according to any one of the previous claims, where a public key method is used for signing, in particular a public key method, in which the sending device (1) has a secret code allocated to it and the receiving device (5) has the corresponding secret code allocated to it.
5. Method according to any one of the previous claims, where the messages between the receiving device (5) and the mobile radio telephone (7) are transmitted by means of the Short-Message-Service (SMS).

6. Method according to any one of the previous claims, where the message (3) is shown before the signing by means of a display device (13) provided in the mobile radio telephone (7).
7. Method according to any one of the previous claims, where the secret code required for the signing is entered through a keyboard device of the mobile radio telephone (7).
8. Method according to any one of the previous claims, where the secret code required for the signing is filed in a chip card of the mobile radio telephone (7), and this code is released by means of a private code (PIN) that can be entered through a keyboard device of the mobile radio telephone (7).

9. Method according to any one of the previous claims, where the chip card carries out the creation of the signed message (9).
10. Method according to any one of the previous claims, where the mobile radio telephone (7) carries out the creation of the signed message (9) and where the secret code is read from the chip card (25).
11. Method according to any one of the previous claims, where the mobile radio telephone (7) additionally serves as a sender for transmitting the signed message (9) to the receiving device (5).
12. Chip card for a mobile radio telephone, where the chip card (25) consists of a signing device (21), which exhibits a storage unit (27) for storing the secret code required for the creation of the signed message (9), characterized in that the signing device (21) creates a signed message (9) from a message (3) to be signed, which was received from the mobile radio telephone (7) through the telephone network.